(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: 0 673 133 A1

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 95200632.8

(51) Int. Cl.6: H04L 9/18

(22) Date of filing: 15.03.95

(30) Priority: 18.03.94 NL 9400428

(43) Date of publication of application:
20.09.95 Bulletin 95/38

(84) Designated Contracting States:
BE CH DE DK ES FR GB GR IE IT LI LU MC PT SE

(71) Applicant: Koninklijke PTT Nederland N.V.
P.O. Box 95321
NL-2509 CH The Hague (NL)

(72) Inventor: De Lange, Martin Klaas
Kersengaarde 188
NL-2272 NN Voorburg (NL)
Inventor: Boly, Jean Paul
Loethe 22
NL-2381 BL Zoeterwoude (NL)

(54) Cryptographic data processing using cascade of cryptographic elements in feedback structure.

(57) The invention provides a device (1) for encrypting or decrypting data packets, comprising storage means (14) for temporarily storing data packets, identification means (15) for identifying data packets, processing means (11, 12, 13) for cryptographically processing data packets, and memory means (16) for storing cryptographic information. The processing means (11, 12, 13) comprise, according to the invention, a first (11) and a second (12) cryptographic element, the first cryptographic element (11) being designed for generating, on the basis of a first starting value, processing data for cryptographically processing a data packet, and the second cryptographic element (12) being designed for generating, on the basis of a second starting value, the first starting value. In addition, the processing means (11, 12, 13) according to the invention are designed for forming, on the basis of a cryptographically processed data packet, the second starting value, thereby ensuring the synchronization between corresponding encrypting and decrypting devices.

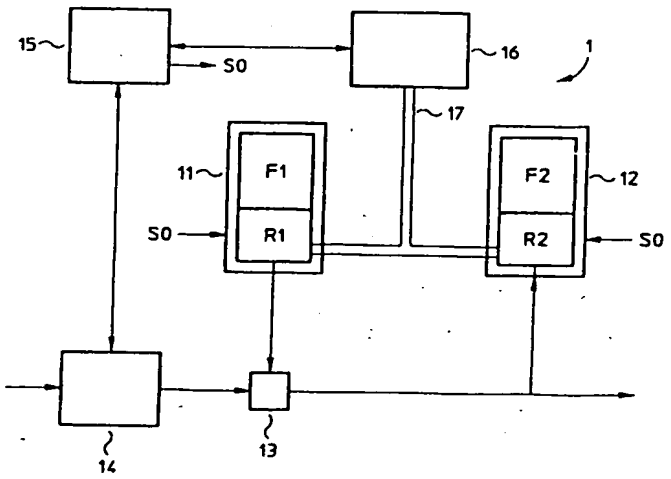

Fig. 1

EP 0 673 133 A1

BACKGROUND OF THE INVENTION

The invention relates to a device for processing data packets, comprising buffer means for temporarily storing data packets, identification means for identifying data packets, processing means for cryptographically processing data packets and memory means for storing cryptographic information. Such a device is disclosed in the US Patent Specification US-5,048,087 (Trbovich et al.).

In the known device, a key and a cryptographic value are stored in a memory for each channel (or virtual connection). Said cryptographic value is the final value (cryptographic residue) of the cryptographic process used after carrying out a cryptographic processing on a data packet. In this method, said final value, that is to say the state (state vector) after the processing steps carried out, is stored in the memory as starting value (initialization vector) for a subsequent data packet of said channel. This repeated use of the final value as new starting value has the disadvantage that the cryptographic security is relatively small because of the traversing (for a particular channel) of a large number of successive states of the cryptographic process concerned, as a cyclic repetition of the states may occur. Furthermore, the device according to the prior art has the disadvantage that, if one or more data packets are lost, the synchronization between encrypting and decrypting device will be lost as well. Thus, the loss of, for example, one data packet on the data connection will always result in the state of the preceding packet being used in the decrypting device for the initialization of the cryptographic function (cryptographic process), as a result of which the "decrypted" data packets will be unrecognizably garbled in most cases.

SUMMARY OF THE INVENTION

The object of the invention is to eliminate the abovementioned disadvantages and other disadvantages of the prior art and to provide a device which offers both a very high cryptographic security and, independently of the cryptographic process used, ensures synchronization of encrypting and decrypting devices, even in the event of the loss of a plurality of data packets.

In addition, the object of the invention is to provide a device for cryptographically processing data packets which is suitable for high data rates, such as the data rate handled in ATM (asynchronous transfer mode) of approximately 155 Mbit/s.

For this purpose, the device according to the invention is characterized in that the processing means comprise a first and a second cryptographic element, the first cryptographic element being designed for generating, on the basis of a first starting value, processing data for the cryptographic processing of a data packet, and the second cryptographic element being designed for generating, on the basis of a second starting value, the first starting value, and that the processing means are designed for forming the second starting value on the basis of a cryptographically processed data packet.

Because the processing means comprise a first and a second cryptographic element, the second cryptographic element providing the starting value of the first element, a very high cryptographic strength can be achieved since the starting values of the first cryptographic element are virtually independent of the preceding final values. In addition, it is possible in this way to design the two elements in a cryptographically simpler way than a comparable single element, as a result of which, firstly, higher processing rates and, secondly, smaller states (state vectors, such as starting and final values) are possible. The smaller starting and final values can, in turn, be retrieved or stored more quickly, and this results in a further increase in rate.

The two cryptographic elements may carry out different cryptographic processes, possibly with different complexities. With a constant cryptographic strength of the device, the complexities of the elements are essentially complementary. According to a preferred embodiment of the invention, however, the cryptographic elements are identical, that is to say they carry out identical cryptographic processes.

Advantageously, the processing means are designed for interchanging the functions of the first cryptographic element and the second cryptographic element. As a result, it is not necessary to transfer starting or final values of one cryptographic element to the other, which makes the processing of very rapidly succeeding data packets possible.

In a preferred embodiment, at least one cryptographic element is provided with plural registers. With the aid of two or more registers per cryptographic element, it is possible to carry out a cryptographic processing, such as the generation of a new final value, on the content of a first register, while at least one other register remains available for temporarily storing a value generated earlier or to be used later, and therefore functions as a buffer. In this case, the registers are advantageously designed for copying the content of a register to another register. In the case of parallel copying, in particular, a rapid transfer of the values to the various registers is therefore possible, as a result of which the processing means are able to shift rapidly to the generation of new values.

The device according to the invention is preferably accommodated in an application-specific integrated circuit (ASIC).

The invention furthermore provides a method of generating cryptographic processing data, comprising carrying out a first cryptographic processing on a first starting value, a final value of the first cryptographic processing being used as processing data, characterized by the carrying out of a second cryptographic processing on a second starting value, a final value of the second cryptographic processing being used as first starting value for the first cryptographic processing, and the second starting value being formed on the basis of a key and data which have been combined with processing data.

REFERENCES

[1] W. Diffie & M. E. Hellman: "Privacy and Authentication: An Introduction to Cryptography", Proceedings of the IEEE, Vol. 67, No. 3, March 1979

[2] EP-A-0,227,318

[3] US-A-5,048,087

[4] NL-A-93,01841

[5] WO-A-87,07796

[6] EP-A-0,366,288

[7] National Bureau of Standards, "Data Encryption Standard", Federal Information Processing Standard, Publication 46, U.S. Dept. of Commerce, January 1977.

[8] Tesa-7, pr. EN 726-2, "Terminal Equipment (TE); Requirements for IC Cards and Terminals for Telecommunication Use - Part 2: Security Framework".

The above references are herewith incorporated in this text.

EXEMPLARY EMBODIMENTS

The invention will be explained in greater detail below by reference to the figures.

Fig. 1 shows diagrammatically a first embodiment of the device according to the invention.

Fig. 2 shows diagrammatically a second embodiment of the device according to the invention.

Fig. 3 shows diagrammatically a third embodiment of the device according to the invention.

Fig. 4 shows diagrammatically a fourth embodiment of the device according to the invention.

Fig. 5 shows diagrammatically a system for the encrypted transfer of data packets, in which the invention is used.

In the encrypting device 1 according to the invention shown diagrammatically and by way of example in Fig. 1, the processing means comprise a first cryptographic element 11, a second cryptographic element 12 and a combination element 13. The buffer means are formed by an input buffer 14. Said input buffer 14 is coupled to an identification unit 15, which forms the identification means. The memory means comprise a memory 16 which is connected to the first cryptographic element 11 and the second cryptographic element 12 by means of a data bus 17. In the embodiment shown, the device is controlled by the identification unit 15, which emits suitable control signals (for example S0) for this purpose. Possibly, however, a separate control unit may be provided. Furthermore, if necessary, an output buffer connected to the combination element 13 may be provided (not shown).

A data packet which arrives in the device 1 is temporarily stored in the input buffer 14 until the identification unit 15 has identified the data packet and the processing means are ready to process the data packet. The identification of a data packet comprises determining the (logical) channel of the data packet, "channel" also being understood here to mean a virtual path or connection of a different type, possibly virtual. In the case of ATM, for example, the identification unit 15 determines the virtual channel or the virtual connection on the basis of the "virtual channel identifier" (VCI) or the "virtual path identifier" (VPI), that is to say on the basis of information present in the header of the data packet. For this purpose, the header of the data packet may be copied from the input buffer 14 to the identification unit 15. In addition to determining the channel, further information may, if necessary, be derived both from the header and from the data field of the data packet.

If the data packet is identified, processing information is read out of the memory 16, for example information which specifies whether data packets of the channel concerned have to be encrypted, decrypted or not processed at all. If a processing of the data packet is necessary, a corresponding key may be read out of the memory 16 on the basis of the (channel) identification. A separate memory (not shown) may also be provided for the purpose of storing keys.

The processing, in the present case encrypting, of a data packet takes place as follows. A starting value (starting vector) associated with the channel concerned, is loaded into the cryptographic element 11 from the memory 16. For this purpose, the element 11 can be conceived as divided up functionally into a register R1 and a cryptographic function F1, it being possible for the register R1 to comprise memory elements, such as flip-flops. The function F1, which is embodied, for example, by a microprocessor and a memory, calculates, in a number of steps, a new cryptographic value (final value) from the starting value. Preferably, like the final value, the starting value has a

length of 256 bits, and the function carries out 48 steps (corresponding to the 48 data bytes of an ATM packet), which successively yields 48 states having associated state vectors (intermediate values). One byte (octet) is successively extracted from each state of 256 bits, which byte forms the "running key" of a corresponding data byte of the data packet. In the combination element 13, the bytes of the running key ("processing bytes") are combined with the data bytes of the data packet. Preferably, this takes place by addition modulo 2 of the corresponding bits, but other operations, such as multiplication, are also possible in principle.

The processing element 11 is preferably designed so that the header of a data packet is not changed. In the case of the bytes of the header for example, this can readily be achieved by modulo 2 addition of processing bytes which comprise only zeros. For this purpose, the identification unit 15 (or, if present, a separate control unit) activates the cryptographic element 11 or the combination element 13 by supplying suitable control signals (for example, S0).

The values of the first eight processed (encrypted) bytes emitted by the combination element 13 are copied to the cryptographic element 12 and stored in a register R2 present for this purpose. In this connection, the register R2 may be constructed from memory elements, such as flip-flops, possibly interlaced with the function F2. In the element 12, said 64 bits are placed one after the other in a total of four copies, which results in a number having a length of 256 bits. For said number, the key of the channel concerned, which also has a length of 256 bits, is added modulo 2. The resulting number functions as starting value (starting vector) for the cryptographic function F2. The final value (final vector), which is stored in the memory 16 and will be used for the function F1 as starting value for the subsequent data packet of the channel concerned, is then calculated in, preferably, 40 steps.

As a result of using only a limited number of bytes, such as the abovementioned first eight bytes, of each processed data packet instead of, for example, all 48 data bytes of an ATM data packet for forming a starting value, the result is achieved that the formation of a new starting value can be started even during the processing of the data packet. It will be clear that the processing rate of the device can be higher as a result of this.

In the device according to the invention, therefore, data of a processed data packet, preferably combined with a key, is used to provide the starting value of a cryptographic process. The final value of said process is used as starting value of another process which generates the running key for the encryption or decryption. In the embodiment shown, a data packet is always encrypted on the basis of a starting value which is determined on the basis of the preceding data packet of that channel. This achieves the result that a minimum number of data packets is incorrectly decrypted in the event of the loss of a data packet at the receiving end. The device according to the invention may also, however, be constructed so that the encrypting of a data packet is determined not as a function of the last data packet of that channel, but as a function of, for example, the penultimate data packet, so that one data packet is passed over. A plurality of data packets may possibly be passed over. In principle, the starting value of the encrypting process can also be based on an earlier data packet of another channel, for example the last data packet encrypted by the device. However, this results in a certain degree of mutual dependence of the channels, which is generally cryptographically undesirable.

In the processing means shown, a combination element 14 is present for combining, for example, a bit stream to be encrypted with an encrypting bit stream. Such a combination element may be formed, for example, by an exclusive-OR gate. It is also possible, however, to construct the processing means in such a way that the cryptographic process of the cryptographic element 11 acts directly on the data of a data packet and does not therefore produce a separate running key. In that case, the separate combination element 13 can be omitted.

The actual cryptographic process used in the cryptographic elements 11 and 12 is, in principle, arbitrary, as long as it produces a cryptographical value based on a starting value. Suitable processes are e.g. the well-known DES algorithm (reference 7) and the RSA algorithm. See also reference 1.

The device 1 of Fig. 1 may be constructed from discrete, commercially available components, but is preferably accommodated, at least partly, in an application-specific integrated circuit (ASIC). The device 1 is suitable not only for rapidly encrypting ATM data packets, but also for processing data packets which are transferred in accordance with other protocols, such as X.25. It will be clear that the given numerical values such as the number of bits in a key, the number of steps of a cryptographic process and the number of bytes to be encrypted, may vary as a function of the specific application or implementation and are given here only by way of example. Although the invention is described here by reference to the processing of data packets, the inventive idea can be used just as well in the processing of data streams not consisting of data packets.

The device 1' according to the invention shown diagrammatically in Fig. 2 largely corresponds to the device 1 of Fig. 1, but is adapted for the

decrypting of data packets. The device 2 also comprises a first cryptographic element 11, a second cryptographic element 12, a combination element 13, an input buffer 14, an identification unit 15, a memory 16, and a data bus 17. In contrast to Fig. 1, the positions of the elements 11 and 12 are interchanged in Fig. 2, that is to say the element 12 is connected to the input buffer 14 and the combination element 13, so that the contents of encrypted data packets are supplied to the element 12. It will be clear that the input buffer 14 of the device 2 receives encrypted data packets and that said data packets are decrypted in the combination element 13, if that is desirable for the channel concerned. The decryption takes place in this case by combining the data of a data packet with a running key. In the case where the data have been encrypted by the addition modulo 2 of a running key, the decryption takes place by the addition modulo 2 of an identical running key.

Fig. 3 shows a device according to the invention which is suitable for both encryption and decryption. The device 1" of Fig. 3 largely corresponds to the devices 1 and 1', respectively, of Fig. 1 and 2. As a departure from Fig. 1 and 2, however, selection means 18 are provided between the cryptographic element 12, on the one hand, and the outputs of the combination element 13 and the input buffer 14, on the other. The supplying of a selection signal S1 to the selection means 18, which may be constructed, for example, of AND gates, connects either the output of the buffer 14 (decryption), or the output of the combination element 13 (encryption) to the cryptographic element 12. The selection signal S1 can be generated either by the identification unit 15 (or a control unit coupled thereto), for example in response to the identification of a channel, or by external means, such as a selection switch (not shown).

In the case of the devices of Fig. 1,2 and 3, a final value has to be written for each data packet into the memory 16, while a starting value has to be retrieved from the memory. In the given example, the length of these values is 256 bits. In the case of very high data rates, such as required in the case of ATM, the timely transfer of the respective starting and final values in the abovementioned embodiments can take place only if very wide data paths (for example, data bus 17) are used, which makes the device relatively expensive. In principle, it is possible to reduce the length of the said values, but this also reduces the cryptographic security. According to a further aspect of the present invention, therefore, different embodiments are provided which make it possible to transfer, even at very high data rates, starting and final values comprising a large number of bits and therefore offering a high cryptographic security.

Firstly, the data bus 17 can be split into two separate data buses 171 and 172 (not shown), the first data bus 171 being connected to the memory 16 and the first cryptographic element 11, while the second data bus 172 is connected to the memory 16 and the second cryptographic element 12. As a result, it is possible to exchange simultaneously information between the memory 16 and the element 11, on the one hand, and the memory 16 and the element 12, on the other. For this purpose, the memory 16 is advantageously constructed so that writing into a first section can take place while reading out from a second section can take place simultaneously. In particular, the memory 16 may be designed for copying information from the second to the first section, so that final values written earlier into the second section can simultaneously be read out from the first section and new final values can be written into the second section.

Secondly, the registers R1 and R2 of the elements 11 and 12 can be constructed in duplicate, so that not only a value on which an operation is being carried out at that instant can be stored in each register, but also a subsequent value. This will be explained in greater detail below by reference to Fig. 4.

Thirdly, the device can be constructed so that the registers R1 and R2 are able to exchange their respective content simply and quickly, for example as a result of the presence of a sufficiently wide data path (data bus) between the registers. This is advantageous, in particular, if two successive data packets to be processed belong to the same channel. For the purpose of this exchange, the elements 11 and 12 can advantageously be constructed in integrated form so that the registers R1 and R2 are arranged in parallel and at a short distance from one another.

Fourthly, the device can be constructed so that the function of the cryptographic elements 11 and 12 can interchange. This will be explained in greater detail by reference to Fig. 4. This, too, is advantageous, in particular, if two successive data packets to be processed belong to the same channel. In this case, the content of the register R2 no longer has to be transferred to the register R1 since R2 takes over the function of R1 as a result of the exchange. In such an embodiment, the cryptographic functions F1 and F2 will generally be identical.

Fifthly, the processing means may be designed for forming the starting value on the basis of a data packet other than the last data packet (of the channel concerned), as already stated above. By "passing over" a data packet in the sense of not using said data packet for forming a starting value, time is gained for writing and reading out information (such as starting and final values). The dis-

advantage of this is that more data packets will be incorrectly decrypted in the event of a loss, that is to say non-arrival or deformed arrival, of a data packet at the receiving end.

Furthermore, according to the non-prepublished Dutch Patent Application NL-A-93,01841, the device may be provided with a plurality of parallel processing means. As a result, a very high processing rate can be achieved, since a plurality of data packets can be processed simultaneously (or virtually simultaneously). Dutch Patent Application NL-A-93,01841 is hereby incorporated by reference in this text.

The encrypting device 1''' according to the invention shown in Fig. 4 is constructed so that a very high processing rate can be achieved even with relatively long starting and final values, however without constructing a plurality of the processing means. The device 1''' of Fig. 4 largely corresponds to the device 1 of Fig. 1, but the processing means are additionally provided with selection means 19, which comprise a first selection element 191 and a second selection element 192. In addition, the registers R1 and R2 in Fig. 4 are constructed in duplicate, as will be explained in greater detail later.

The selection means 19 offer the possibility of interchanging the functions of the cryptographic elements 11 and 12. For this purpose a first input of the selection element 191 is connected to the register R1 and a second input to the register R2, while the output is connected to the combination element 13. A selection signal S2, which connects either the register R1 or the register R2 to the combination element 13, can be supplied to a control input of the selection element 191. In a comparable way, the input of the selection element 192 is connected to the output of the combination element 13 and the outputs of the selection element 192 are connected to the register R1 and the register R2, respectively. The output of the combination element 13 can be connected either to the register R1 or to the register R2 by supplying a selection signal S2 to a control input. Depending on the selection signal S2, the operation of the device of Fig. 4 will therefore, in a first mode, correspond completely with that of Fig. 1. In a second mode, the cryptographic elements are functionally interchanged with respect to Fig. 1, so that the function F1 determines the starting value of the function F2 and the final value of the function F2 is supplied to the data to be processed. The selection signal S2 may be generated in the identification unit 15 or in a separate control unit (not shown). Preferably, the selection signal S2, or a signal related thereto, is also supplied to the cryptographic elements 11 and 12 and to the memory 16 in order to ensure that the correct information (such as starting and final values and keys) is transferred to the correct element.

The functional interchange of the cryptographic elements makes it possible in the case of data packets of the same channel which are to be processed successively to supply very rapidly the final value of one function (for example F1) as starting value to the other function (for example F2). No transfer of said value from one register (for example R1) to the other register (for example R2) therefore needs to take place. As a result, very large values, that is to say having a large bit length and therefore having a high cryptographic security, can be used.

If two successive data packets belong to different channels, in most applications the final value of one function (for example F2) cannot directly be used as starting value by the other function (for example, F1) so that said final value has to be stored. In order to avoid delay as a consequence of congestion on the data bus 17 or limited access times of the memory 16, the device of Fig. 4 is provided with double registers, which offer the possibility of temporarily storing a second value. For this purpose, the register R1 comprises a section R1a and a section R1b, both sections preferably being capable of containing an entire starting or final value (in the above example, 256 bits). The register R2 likewise comprises a section R2a and a section R2b. If, for example, the device is now operating in the first mode (according to Fig. 1) and two successive data packets belong to different channels, a final value which has to be stored in the memory 16 will be present in the register R2, for example in the section R2a, after the encrypting of the first packet. At very high data rates, the time between two data packets may be insufficient to transfer the, for example, 256 bits of said value to the memory 16. For this reason, in the embodiment of Fig. 4, the content of one register section (for example R2a) can be copied to the other register section (for example, R2b). This releases one register (R2a) for receiving and processing fresh data, while the final value determined can be transferred from the other section (R2b) to the memory 16. As a result, the transfer via the data bus 17 and the determination of a fresh value can take place simultaneously. As an alternative to copying from one register section to the other register section, the operation elements can be constructed so that the register sections are alternatingly connected to the corresponding function (F1 or F2) or to the data bus 17 and the inputs and outputs of the respective cryptographic elements. For this purpose, like the selection means 19 shown in Fig. 4, internal selection means may be provided for the processing means.

It will be clear that the additional measures shown in Fig. 4 can also be used separately, for example by constructing the registers R1 and R2 in duplicate without carrying out a functional interchange of the elements 11 and 12. Characteristics of the device of Fig. 4 may also be combined with, for example, the device 1'' of Fig. 3.

The communication system 9 shown in Fig. 5 comprises a network 91, to which a plurality of security units 92 are connected. An end user 93 is connected to each security unit 92. The network 91 is, for example, an ATM network and the end users 93 are, for example, digital telephone sets, data terminals and/or payment terminals. Each security unit 92 comprises at least one encrypting device 1 and one decrypting device 1' according to the invention, or a combined device 1'' as shown in Fig. 3, a device 1''' as shown in Fig. 4, or another embodiment of the device according to the present invention. The system 9 constructed in accordance with the invention makes possible a rapid, secure transfer of data packets.

It will be understood by those skilled in the art that the invention is not limited to the exemplary embodiments shown and that many modifications and additions are possible without departing from the spirit and scope of the present invention.

Claims

1. Device (1; 1'; 1''; 1''') for cryptographically processing data packets, comprising:
   - buffer means (14) for temporarily storing data packets,
   - identification means (15) for identifying data packets,
   - processing means (11, 12, 13) for cryptographically processing data packets, and
   - memory means (16) for storing cryptographic information,

   characterized in that
   - the processing means comprise a first (11) and a second (12) cryptographic element, the first cryptographic element (11) being designed for generating, on the basis of a first starting value, processing data for the cryptographic processing of a data packet, and the second cryptographic element (12) being designed for generating, on the basis of a second starting value, the first starting value, and in that
   - the processing means are designed for forming the second starting value on the basis of a cryptographically processed data packet.

2. Device according to claim 1, wherein the processing means are designed for encrypting data packets.

3. Device according to claim 1, wherein the processing means are designed for decrypting data packets.

4. Device according to claims 2 and 3, wherein the processing means are designed for optionally encrypting or decrypting data packets.

5. Device according to any of the preceding claims, designed for processing data packets from different logical channels and for storing in the memory means (16), for each channel, a key and/or a first starting value.

6. Device according to any of the preceding claims, wherein the processing means comprise a combination element (13) for combining processing data with data of data packets to be processed, the combination element (13) preferably comprising a modulo-2 adder.

7. Device according to any of the preceding claims, wherein the first cryptographic element (11) and the second cryptographic element (12) are designed for carrying out identical cryptographic functions.

8. Device according to claim 7, wherein the processing means are designed for interchanging the functions of the first cryptographic element (11) and the second cryptographic element (12).

9. Device according to any of the preceding claims, wherein the processing means are designed for forming the second starting value on the basis of a key and the first eight bytes of a processed data packet.

10. Device according to any of the preceding claims, wherein the processing means are designed for directly exchanging values between the cryptographic elements (11, 12).

11. Device according to any of the preceding claims, wherein at least one cryptographic element (e.g. 11) is provided with plural registers (e.g. R1a, R1b).

12. Device according to claim 11, wherein the registers are designed for copying the content of one register (e.g. R1a) to another register (e.g.R1b).

13. Device according to any of the preceding claims, provided with at least two parallel processing means.

14. Device according to any of the preceding claims, suitable for processing ATM cells.

15. Device according to any of the preceding claims, accommodated in an integrated circuit.

16. Method of generating cryptographic processing data, comprising carrying out a first cryptographic processing on a first starting value, a final value of the first cryptographic processing being used as processing data, characterized by the carrying out of a second cryptographic processing on a second starting value, a final value of the second cryptographic processing being used as first starting value for the first cryptographic processing, and the second starting value being formed on the basis of a key and data which have been combined with processing data.

17. System (9) for transferring data by means of encrypted data packets, comprising at least one device (92; e.g. 1, 1') according to any of claims 1 to 15 inclusive.

18. System (9) according to claim 17, designed for transferring data packets in accordance with the asynchronous transfer mode (ATM).

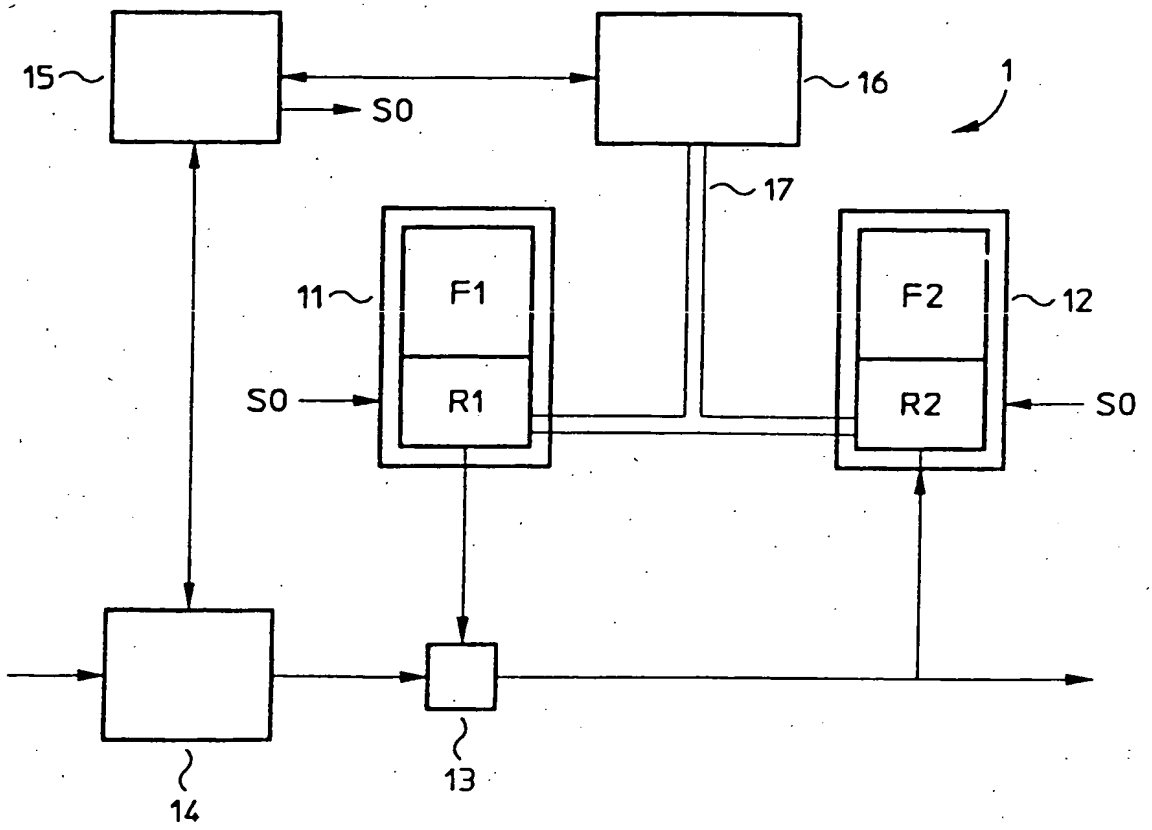

Fig. 1

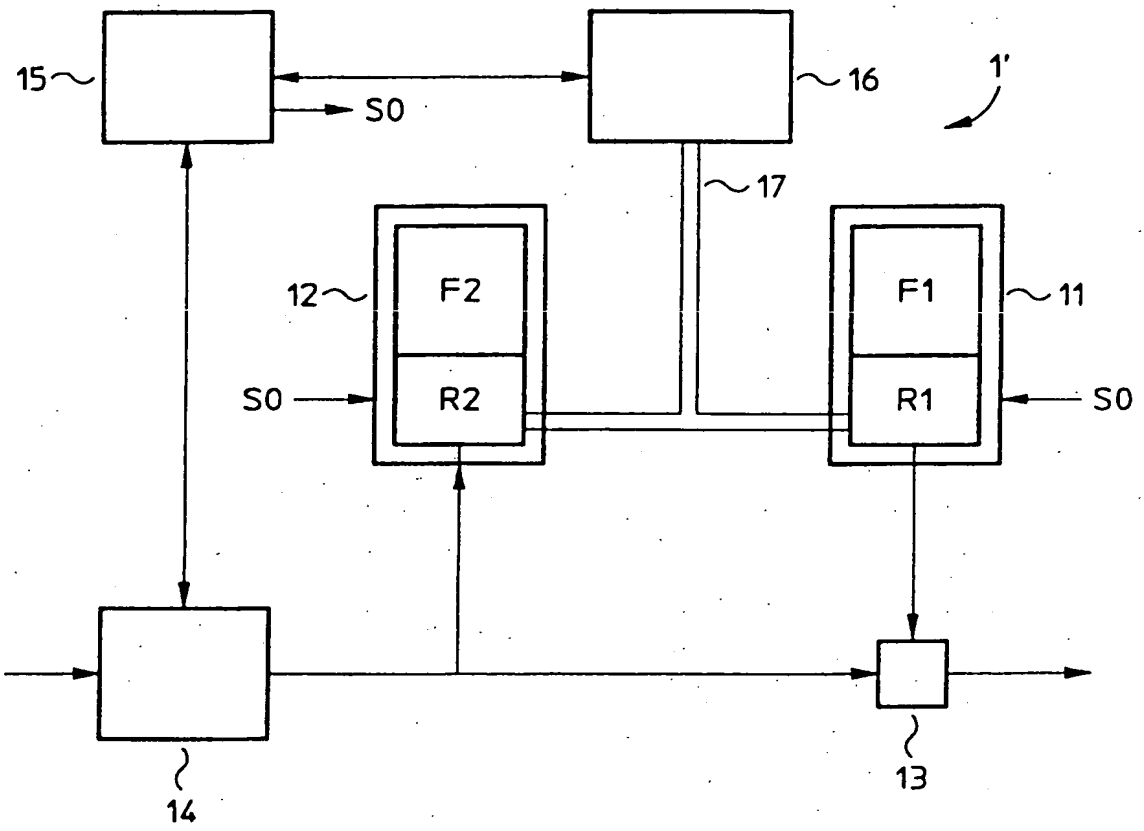

Fig. 2

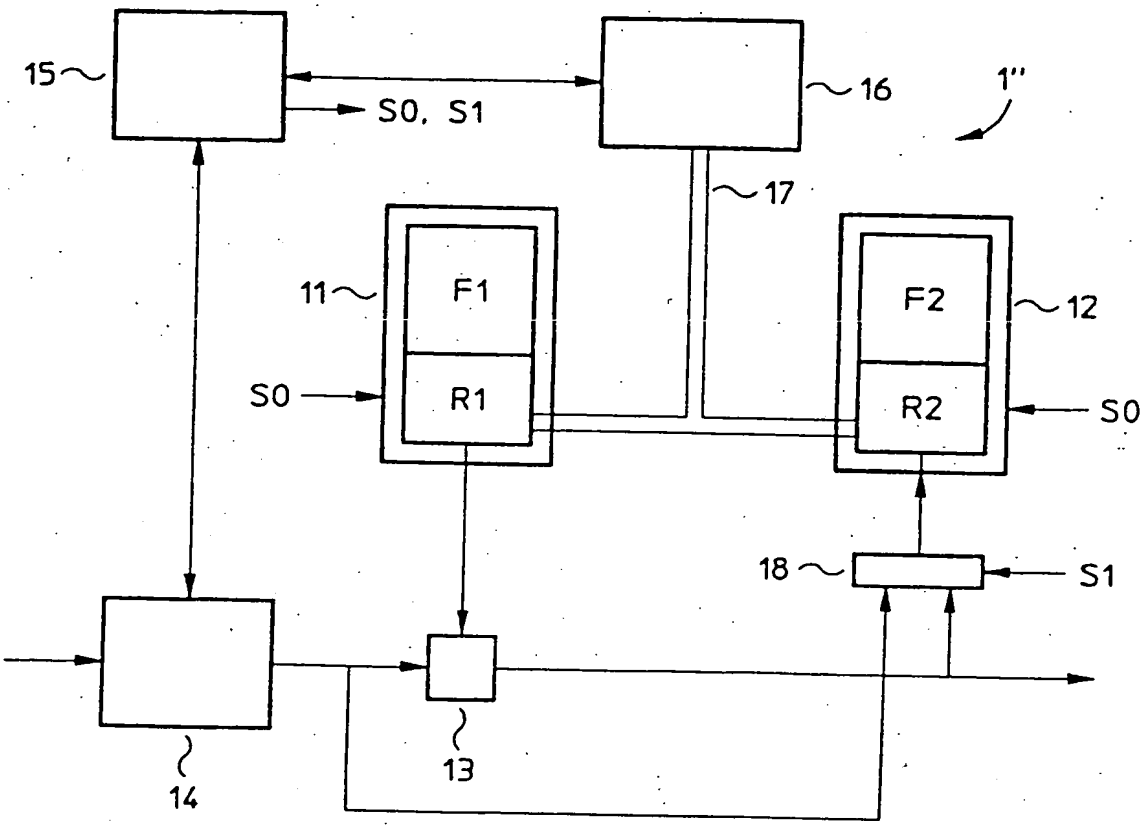

Fig. 3

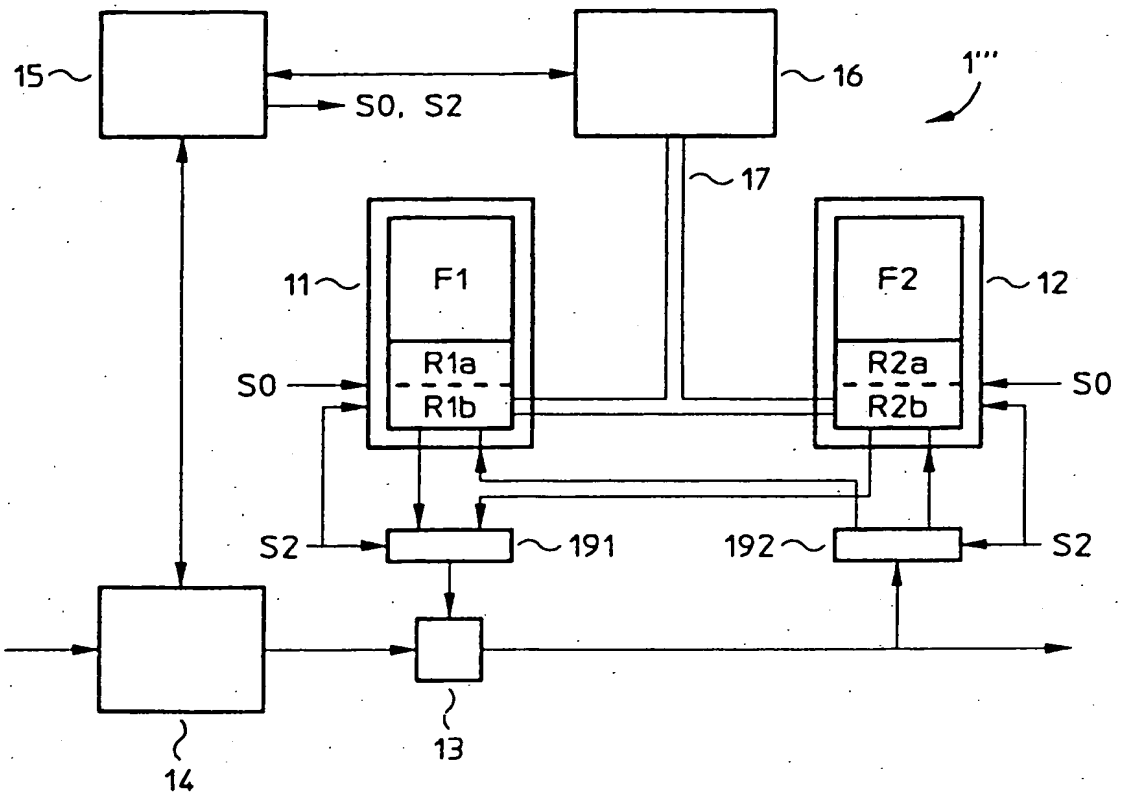

Fig. 4

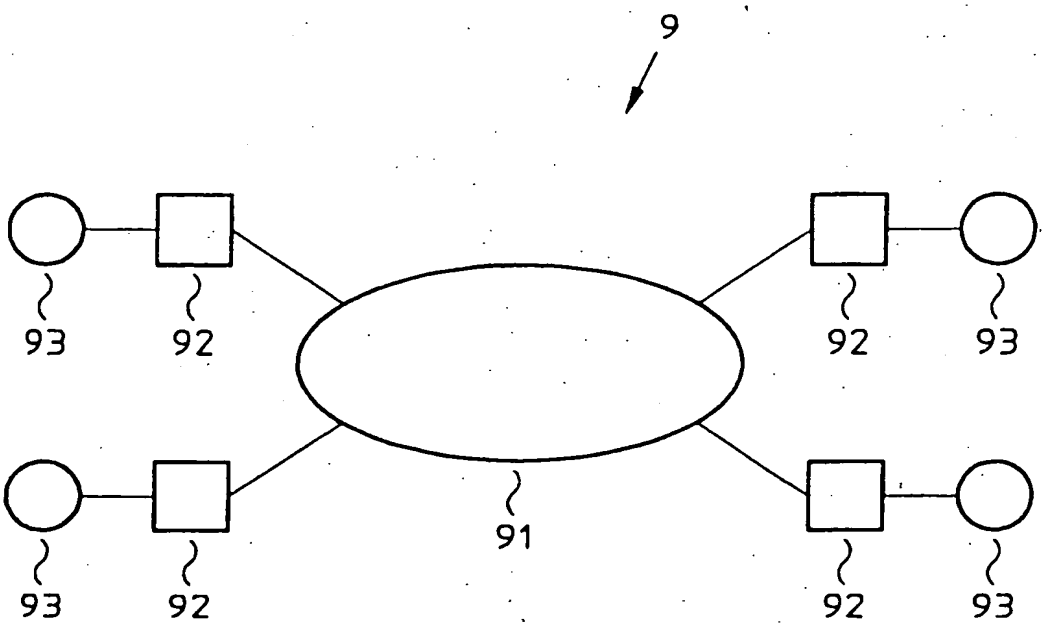

Fig. 5

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 95 20 0632

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	WO-A-87 07796 (DATAKONSULT I MALMÖ AB) 17 December 1987	16,17	H04L9/18
A	* page 11, line 9 - page 12, line 2; figure 3 * * page 7, line 33 - page 8, line 15; figure 1 *	1,6,7	
A	EP-A-0 366 288 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2 May 1990 * abstract *	1	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)
H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	26 June 1995	Bossen, M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)